在以太局域网内数据包传输依靠的是MAC地址，IP地址与MAC对应的关系依靠ARP表，每台主机（包括网关）都有一个ARP缓存表。在正常情况下这个缓存表能够有效的保证数据传输的一对一性，也就是说主机A与主机C之间的通讯只通过网关1和网关1，象主机B之类的是无法截获A与C之间的通讯信息的。但是在ARP缓存表的实现机制中存在一个不完善的地方，当主机收到一个ARP的应答包后，它并不会去验证自己是否发送过这个ARP请求，而是直接将应答包里的MAC地址与IP对应的关系替换掉原有的ARP缓存表里的相应信息。这就导致主机B截取主机A与主机C之间的数据通信成为可能。

首先主机B向主机A发送一个ARP应答包说192.168.1.1的MAC地址是03-03-03-03-03-03，主机A收到这个包后并没有去验证包的真实性而是直接将自己ARP列表中的192.168.1.1的MAC地址替换成03-03-03-03-03-03，同时主机B向网关1发送一个ARP响应包说192.168.1.2的MAC是03-03-03-03-03-03，同样网关1也没有去验证这个包的真实性就把自己ARP表中的192.168.1.2的MAC地址替换成03-03-03-03-03-03。当主机A想要与主机C通讯时，它直接把应该发送给网关1(192.168.1.1)的数据包发送到03-03-03-03-03-03这个MAC地址，也就是发给了主机B，主机B在收到这个包后经过修改再转发给真正的网关1，当从主机C返回的数据包到达网关1后，网关1也使用自己ARP表中的MAC，将发往192.168.1.2这个IP地址的数据发往03-03-03-03-03-03这个MAC地址也就是主机B，主机B在收到这个包后再转发给主机A完成一次完整的数据通讯，这样就成功的实现了一次ARP欺骗攻击。